

## CERTIFICATION

I, Kohno Takao; 4-3 Tsurigane-cho, 2-chome, Chuo-ku, Osaka 540-0035 JAPAN, hereby certify that each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement.

  
\_\_\_\_\_  
**KOHNO Takao**

**Dated this 15th day of May, 2009**

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-047946

(43)Date of publication of application : 18.02.2000

(51)Int.Cl.

G06F 12/14

(21)Application number : 10-212357

(71)Applicant : OKI ELECTRIC IND CO LTD

(22)Date of filing : 28.07.1998

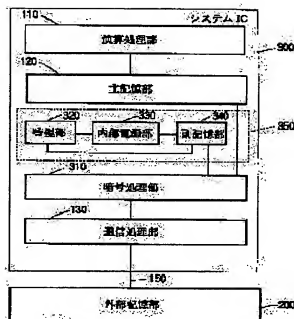
(72)Inventor : JINNAI HIDEOTO  
FUJII TAMOTSU

## (54) INTEGRATED CIRCUIT DEVICE

## (57)Abstract:

**PROBLEM TO BE SOLVED:** To provide an integrated circuit device capable of keeping the safety of a system from the threat of illegal use by analyzing/falsifying a program or data.

**SOLUTION:** A code processing part 310 for decoding the program or data from an external storage part 200 and encoding the data when writing the data into the external storage part 200, a monitoring part 320 for monitoring access from the outside to a system IC 300, an internal power source part 330 having a function for supplying power to a sub storage part 340 and monitoring part 320 and cutting the supply of power to a sub storage part 340 when there is a power supply cutting indication from the monitoring part 320, and the sub storage part 340 for holding an encoding/decoding key based on the supply of power from the internal power source part 330 are integrated in the system IC 300 and these components are made into one chip.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2000-47946  
(P2000-47946A)

(43) 公開日 平成12年2月18日 (2000.2.18)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	キーワード (参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 D 5 B 0 1 7

審査請求 未請求 請求項の数 6 O L (全 8 頁)

(21) 出願番号 特願平10-212357

(22) 出願日 平成10年7月28日 (1998.7.28)

(71) 出願人 000000295  
沖電気工業株式会社  
東京都港区虎ノ門1丁目7番12号

(72) 発明者 陣内 秀人  
東京都港区虎ノ門1丁目7番12号 沖電気  
工業株式会社内

(72) 発明者 藤井 保  
東京都港区虎ノ門1丁目7番12号 沖電気  
工業株式会社内

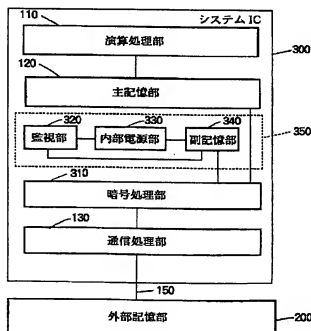
(74) 代理人 100083840  
弁理士 前田 実  
Fターム (参考) 5B017 AA01 AA07 BA07 BA08 BB03  
CA13 CA14

(54) 【発明の名称】 集積回路装置

(57) 【要約】

【課題】 プログラムやデータの解析・改竄による不正な使用の脅威からシステムの安全を保持することのできる集積回路装置を提供する。

【解決手段】 システムIC 300は、外部記憶部200からのプログラムやデータを復号化するとともに、外部記憶部200にデータを書き出す時にデータの暗号化を行う暗号処理部310と、システムIC 300に対する外部からのアクセスを監視する監視部320と、副記憶部340及び監視部320に電源を供給し、監視部320から電源遮断指示があると副記憶部340への電源供給を遮断する機能を有する内部電源部330と、内部電源部330の電源供給により暗号化鍵/復号化鍵を保持する副記憶部340とをを組み、かつこれらを1チップ化して構成する。



システム IC の構成図

## 【特許請求の範囲】

【請求項 1】 演算処理部、主記憶部、通信制御を行う通信処理部を備え、外部記憶装置とアクセス可能な集積回路装置において、前記外部記憶装置からのプログラム及びデータを復号化するとともに、前記外部記憶装置にデータを書き出す時にデータの暗号化を行う暗号処理部と、内部電源部の電源供給により暗号化鍵／復号化鍵を保持する副記憶部と、集積回路装置に対する外部からのアクセスを監視し、不正アクセスを検知すると電源遮断指示する監視部と、前記副記憶部に電源を供給し、前記監視部から電源遮断指示があると前記副記憶部への電源供給を遮断する機能を有する内部電源部とを備えたことを特徴とする集積回路装置。

【請求項 2】 演算処理部、主記憶部、通信制御を行う通信処理部を備え、外部記憶装置とアクセス可能な集積回路装置において、前記外部記憶装置からのプログラム及びデータを復号化するとともに、前記外部記憶装置にデータを書き出す時にデータの暗号化を行う暗号処理部と、暗号化鍵／復号化鍵を保持する副記憶部と、集積回路装置に対する外部からのアクセスを監視し、不正アクセスを検知すると前記副記憶部の記憶内容を書き換える監視部とを備えたことを特徴とする集積回路装置。

【請求項 3】 前記不正アクセスは、集積回路装置に対して外部からの読み出し／書き込みが通常と異なるアクセスであることを特徴とする請求項 1 又は 2 の何れかに記載の集積回路装置。

【請求項 4】 前記不正アクセスは、集積回路装置に設置された不正検知センサによる検知信号の入力であることを特徴とする請求項 1 又は 2 の何れかに記載の集積回路装置。

【請求項 5】 請求項 1 記載の集積回路装置において、前記暗号処理部、前記副記憶部、前記監視部及び前記内部電源部は、集積回路装置内に組み込みチップ化して構成されたことを特徴とする集積回路装置。

【請求項 6】 請求項 1、2、3、4 又は 5 の何れかに記載の集積回路装置において、集積回路装置は、電子マネーシステムの電子マネーの決済部に用いられる IC であることを特徴とする集積回路装置。

## 【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、集積回路装置に係り、特に、電子マネーシステムの電子マネーの決済部に用いられる集積回路装置に関する。

【0002】

【従来の技術】 エレクトロニク・コマース (Electronic Commerce: 電子商取引) では、現金通貨が有する決済機能 (買手から売手へ経済価値を移転する機能) を、電子マネーという電子的な通貨情報 (以下、電子マネー情報という。) で代替している。

【0003】 一般に、電子マネーを決済手段として機能させるためには、銀行等の金融機関を介在させないで、電子マネーを流通させる IC カード型の電子マネーシステム、あるいは銀行による決済を取引に介在させ、電子マネー情報をオンラインで決済するネットワーク型の電子マネーシステムのいずれかが構築されていなければならない。前者の電子マネーシステムでは、IC カードにデジタルデータとして電子マネー情報を記録して、それを通貨情報として書き換えていくことができる。この電子マネーシステムで使用されるマネーカードは、通信機能、携帯機能、計算機能、及び管理機能等、種々の機能を有する。この結果、現金通貨に比較すると、電子マネー情報を記録した IC カードは、その情報をネットワークを介して遠隔地に瞬時に送れる、電子財布に入れておけば、かさばらずに携帯できる、売上の計算が簡単に行える、いつでも使ったか等の記録がとれる等のメリットがある。

【0004】 今日、実験的に運用されている IC カード型の電子マネーカードシステムは、データの偽造や改竄等の脅威から、個別の金融機関の決済機構と連動されている。したがって、金融機関と利用者との間の資金の移動や、利用者相互間における資金の移動のために IC カード (電子マネーカード) を発行し、また、電子マネーカードへの電子マネーの出入、電子マネーカードから電子マネーの入金、各口座間の振替処理等を管理するために、マネー管理センタが必要とされている。また、後者のネットワーク型の例としては、銀行間等のネットワークによる電子決済があり、セキュリティを確保するために専用回線を介して運用されている。

【0005】 また、電子マネーの発行機関と契約を行った加盟店は、簡易決済端末が設置され、店頭での小口決済が可能となる。すなわち、加盟店は買物代金の決済時に、簡易決済端末に利用者の IC カードを挿入し、売上げ金額を入力することにより簡易決済端末の内蔵 IC カードへ該当金額の価値を移して決済を行う。このように、利用者 IC カードから端末内 IC カードへの電子マネーの移転、または利用者 IC カードからフレット (電子財布) 内 IC カードに集金された電子マネーの端末内 IC カードへの移転を実現する。

【0006】 電子マネーの決済端末としては、例えば図 5 に示すものがある。

【0007】 図 5 は電子マネーの決済部として用いられる従来のシステム IC (集積回路装置) の構成を示す図である。

【0008】 図 5 において、100 は決済端末内部に設

けられ、ICカードにアクセス可能なシステムIC、200はシステムIC100の外部に設置されシステムIC100にデータを提供するRAM、ROM等の外部記憶部、150はシステムIC100と外部記憶部200とを接続する信号線である。

【0009】システムIC100は、CPU等からなる演算処理部110と、高速動作可能なキャッシュメモリ等からなる主記憶部120と、バス制御及び外部との通信制御を行う通信処理部130とから構成される。また、システムIC100を動作させるプログラムやシステムIC100で処理するデータはシステムIC100

の中にはない外部記憶部200に格納している。

【0010】システムIC100は、外部記憶部200から一度取り寄せたデータを主記憶部120に記憶し、次回からの読み出しの際は、主記憶部120にキャッシュされた情報を読み出すことでデータを再度取り寄せなくてもよいようにするキャッシュ機能を有する。

【0011】以上の構成において、システムIC100は、立ち上げ時に通信処理部130が外部記憶部200から信号線150上を通してプログラムを主記憶部120に読み込み、演算処理部110は主記憶部120のプログラムによって動作を開始する。処理するデータは外部記憶部200から通信処理部130を経由してプログラムを主記憶部120に読み込み、演算処理部110は主記憶部120のデータをプログラムにより指定された方法でデータ処理した後、外部記憶部200に書き込む。

#### 【0012】

【発明が解決しようとする課題】しかしながら、このような従来のシステムICにあつては、以下のような問題点があつた。

【0013】すなわち、従来のシステムICでは、動作するプログラムをシステム上でなく外部記憶部200上に記憶しているため、第三者に外部記憶部200からプログラムを読み出されたり、外部記憶部200とシステムIC間の信号線150上を通信するプログラムを読み取れることでプログラムを解析・改竄されシステムを不当に使用される危険がある。

【0014】また、データについても外部記憶部200に記憶しているため、外部記憶部200からデータを読み出されたり、外部記憶部200とシステムIC間の信号線150上を通信するデータを読み取れることでデータを改竄され不正なデータ処理に使用される危険がある。

【0015】本発明は、プログラムやデータの解析・改竄による不正な使用の脅威からシステムの安全を保持することのできる集積回路装置を提供することを目的とする。

#### 【0016】

【課題を解決するための手段】本発明に係る集積回路装

置は、演算処理部、主記憶部、通信制御を行う通信処理部を備え、外部記憶装置とアクセス可能な集積回路装置において、外部記憶装置からのプログラム及びデータを復号化するとともに、外部記憶装置にデータを書き出す時にデータの暗号化を行う暗号処理部と、内部電源部の電源供給により暗号化鍵／復号化鍵を保持する副記憶部と、集積回路装置に対する外部からのアクセスを監視し、不正アクセスを検知すると電源遮断指示する監視部と、副記憶部に電源を供給し、監視部から電源遮断指示があると副記憶部への電源供給を遮断する機能を有する内部電源部とを備えて構成する。

【0017】本発明に係る集積回路装置は、演算処理部、主記憶部、通信制御を行う通信処理部を備え、外部記憶装置とアクセス可能な集積回路装置において、外部記憶装置からのプログラム及びデータを復号化するとともに、外部記憶装置にデータを書き出す時にデータの暗号化を行う暗号処理部と、暗号化鍵／復号化鍵を保持する副記憶部と、集積回路装置に対する外部からのアクセスを監視し、不正アクセスを検知すると副記憶部の記憶内容を書き換える監視部とを備えて構成する。

【0018】上記不正アクセスは、集積回路装置に対して外部からの読み出し／書き込みが通常と異なるアクセスであってもよく、また、上記不正アクセスは、集積回路装置に設置された不正検知センサによる検知信号の入力であってもよい。

【0019】本発明に係る集積回路装置は、暗号処理部、副記憶部、監視部及び内部電源部が、集積回路装置内に組込み1チップ化して構成されたものであつてもよく、また、本発明に係る集積回路装置は、電子マネーシステムの電子マネーの決済部に用いられるICであってもよい。

#### 【0020】

【発明の実施の形態】本発明に係る集積回路装置は、電子マネーシステムの電子マネーの決済部に用いられるシステムICに適用することができる。

#### 【0021】第1の実施形態

図1は本発明の第1の実施形態に係る集積回路装置の構成を示すブロック図である。本実施形態に係る集積回路装置の説明にあたり前記図5と同一構成部分には同一符号を付している。

【0022】図1において、300は決済端末内部に設けられICカードにアクセス可能なシステムIC（集積回路装置）、200はシステムIC300の外部に設置されシステムIC300にデータを提供するRAM、ROM等の外部記憶部（外部記憶装置）、150はシステムIC300と外部記憶部200とを接続する信号線である。

【0023】システムIC300は、CPU等からなる演算処理部110と、高速動作可能なキャッシュメモリ等からなる主記憶部120と、バス制御及び外部との通

信制御を行う通信処理部 130 と、外部記憶部 200 からのプログラムやデータを復号化するとともに、外部記憶部 200 にデータを書き出す時にデータの暗号化を行う暗号処理部 110 と、システム 1C300 に対する外部からのアクセスを監視する監視部 320 と、副記憶部 340 及び監視部 320 に電源を供給し、監視部 320 から電源遮断指示があると副記憶部 340 への電源供給を遮断する機能を有する内部電源部 330 と、内部電源部 330 の電源供給により記憶内容（暗号化鍵／復号化鍵）を保持する副記憶部 340 とから構成される。

【0024】システム 1C300 を動作させるプログラムやシステム 1C300 で処理するデータは、暗号化されたデータとして外部記憶部 200 に保管されている。また、システム 1C300 は、外部記憶部 200 から一度取り寄せた暗号化データを、復号化して主記憶部 120 に記憶し、次回からの読み出す際は、主記憶部 120 にキャッシュされた情報を読み出すことでデータを再度取り寄せなくてもよいようにするキャッシュ機能を有する。

【0025】システム 1C300 と外部記憶部 200 の間は従来例と同様に信号線 150 により接続されているが、信号線 150 上を経由するプログラムや処理データは全て暗号化されている。

【0026】上記監視部 320、内部電源部 330 及び副記憶部 340 は、全体として監視手段 350 を構成する。

【0027】図 2 は上記監視手段 350 の構成を詳細に示すブロック図である。

【0028】図 1 及び図 2 において、暗号処理部 310 は、外部記憶部 200 のプログラムを読み込む場合やデータを読み込む時に復号化し、外部記憶部 200 にデータを書き出す時にデータの暗号化を行う。暗号化／復号化に使用する暗号化鍵／復号化鍵は、監視手段 350 の副記憶部 340 に記憶されている。

【0029】副記憶部 340 は、暗号化／復号化に使用する暗号化鍵／復号化鍵として、公開鍵暗号方式である RSA 方式と秘密鍵方式である DES (Data Encryption Standard)、FEAL 等を併用する。例えば、暗号化鍵として、例えば 64 bit の DES を用いるとともに、暗号処理の基本方式としてプログラム、データ、その他の部分の暗号処理は、異なる方式をとる。また、暗号処理は、副記憶部 340 の暗号化鍵／復号化鍵を使用した暗号処理部 130 が、システム 1C300 内において行う。

【0030】監視部 320 は、マイクロプロセッサ等により構成され、システム 1C300 に対する外部からのアクセスを常に監視し、システム 1C300 に対して不正なアクセスがあった時、内部電源部 330 に電源遮断指示を出して副記憶部 340 への電源供給を遮断させ、副記憶部 340 の暗号化鍵／復号化鍵を消去する。

【0031】ここで、上記不正なアクセスには、システム 1C300 に対して外部からの読み出し／書き込みが通常と異なるアクセスを判別した場合と、システム 1C300 に設置されたセンサから不正アクセス信号が入力された場合とがある。前者、すなわちシステム 1C300 に対する外部からの読み出し／書き込みが通常と異なるアクセスである場合には、システム 1C300 に対して外部からプログラムやデータの解析・改竄のためのアクセスが行われた可能性があるとして判断して内部電源部 330 に電源遮断指示を出力する。

【0032】また、システム 1C300、特に監視手段 350 を収容する筐体には、該筐体内部を開けたり衝撃を感知したときに応答するセンサが設置されており、センサ出力は監視部 320 に入力されている。上記後者は、このセンサから不正アクセス信号が入力された場合であり、このセンサ入力があった場合には、システム 1C300 を外部から物理的にアクセス（破壊）してプログラムやデータの解析・改竄を行う場合であると判断して内部電源部 330 に電源遮断指示を出力する。

【0033】内部電源部 330 は、副記憶部 340 及び監視部 320 に電源を供給し、監視部 320 から電源遮断指示があると副記憶部 340 への電源供給を遮断する。

【0034】副記憶部 340 は、暗号化／復号化に使用する暗号化鍵／復号化鍵を記憶するもので、内部電源部 330 の電源供給により内容を保持する半導体メモリ（例えば、DRAM）からなる。副記憶部 340 は、内部電源部 330 からの電源供給が絶たれると、極めて短い時間に記憶内容が消失する。

【0035】本実施形態に係るシステム 1C300 は、システム 1C300 内に暗号処理部 110、監視部 320、内部電源部 330 及び副記憶部 340 を組み込み、かつこれらが 1チップ化されて構成されている。したがって、これら回路部を単独で取り出すことは極めて困難であるとともに、暗号化鍵／復号化鍵を記憶する副記憶部 340 は内部電源部 330 によりバックアップされ、監視部 320 が不正アクセスを検知すると前記バックアップを遮断して副記憶部 340 の内容を消去する。

【0036】以下、上述のように構成されたシステム 1C300 の動作を説明する。

【0037】【全体動作】システム 1C300 は、立ち上げ時の動作は通信処理部 130 がプログラムを外部記憶部 200 から暗号化された状態で読み込む。読み込まれたプログラムは、副記憶部 340 に記憶されている復号化鍵を使用して暗号処理部 130 で復号化され、主記憶部 120 に書き込まれる。演算処理部 110 は、主記憶部 120 からプログラムを読み込み、プログラムを実行する。

【0038】システム 1C300 で処理するデータは、外部記憶部 200 に暗号化された状態で記憶されてい

る。システム 1C300 がデータを読み込む場合は、まず通信処理部 130 が通信線 150 を通して外部記憶部 200 からデータを読み込み、読み込んだデータを暗号処理部 310 が副記憶部 340 に記憶されている復号化鍵を使用して復号化する。復号化したデータは主記憶部 120 に書き込まれる。

【0043】演算処理部 110 は、主記憶部 120 に格納されたプログラムによりデータを処理する。

【0044】演算処理部 110 で処理されたデータは暗号処理部 310 に出力され、暗号処理部 310 が副記憶部 340 に記憶された暗号化鍵を使用して暗号化する。暗号化したデータは、通信処理部 130 により通信線 150 を通して外部記憶部 200 に書き込まれる。

【0041】〔監視部 320 の監視動作〕システム 1C300 は、未使用時内部電源部 330 によりバックアップされ、監視部 320 が外部からのアクセスを監視している。監視部 320 の監視により、システム 1C300 に対して外部から通常と異なったアクセス（不正アクセス）があった場合には、監視部 330 は、内部電源部 330 に電源遮断指示を出して副記憶部 340 への電源供給を遮断させ、副記憶部 340 の暗号化鍵／復号化鍵を強制的に消去する。これにより、鍵の盗難を防止する。上記不正アクセスには、前述したように通常と異なる手順や不当なアドレス指定によるアクセスの他、システム 1C300 に設置されたセンサからの入力がある。

【0042】また、内部電源部 330 から供給される電圧が所定値以下となったときも安全性を確保するため、監視部 330 が、内部電源部 330 に電源遮断指示を出して副記憶部 340 への電源供給を遮断させ、副記憶部 340 のデータを消去する。すなわち、内部電源部 330 は規定の使用期間及び通常の使用状態・方法の範囲では、一定電圧を出力するように構成されており、この出力電圧が所定値以下となったときは内部電源部 330 自身が消耗した時を含め安全性の確保が図れなくなった状態であるので、監視部 330 が副記憶部 340 のデータを消去する。

【0043】図 3 は監視手段 350 の監視部 320 の監視動作を示すフローチャートであり、監視部 320 のプロセスにより所定タイミングで繰り返し実行される。図中、ST はフローの各ステップを示す。

【0044】ステップ ST1 に示される状態は、システム 1C300 のイベント待ち状態である。このイベント待ち状態において、内部電源部 330 の出力電圧のチェックを行い、内部電源部 330 の出力電圧が所定値より大きければ内部電源部 330 について異常はないと判断してステップ ST2 に進み、出力電圧が所定値以下のときは内部電源部 330 に異常があると判断してステップ ST5 に進む。

【0045】ステップ ST2 では、システム 1C300 に対する外部からのデータをチェックし、システム 1C

300 に対して外部からの読み出し／書き込みに不正アクセスがないときはステップ ST3 でセンサ入力是否正常かを判別する。

【0046】センサ入力が正常であるときは不正使用がないと判断してステップ ST4 で該当処理を行ってステップ ST1 に戻り上記処理を繰り返す。

【0047】一方、上記ステップ ST1 で内部電源部 330 の出力電圧が所定値以下のとき、上記ステップ ST2 で不正アクセスがあったとき、あるいは上記ステップ ST3 でセンサ入力に異常があったときは、システム 1C300 に対して外部からプログラムやデータの解析・改竄のための不正使用が行われたと判断して内部電源部 330 に電源遮断を指示し、内部電源部 330 から副記憶部 340 への電源供給を遮断する。これにより、副記憶部 340 内の暗号化鍵／復号化鍵を消去する。

【0048】以上説明したように、第 1 の実施形態に係るシステム 1C300 は、外部記憶部 200 からのプログラムやデータを復号化するとともに、外部記憶部 200 にデータを書き出す時にデータの暗号化を行う暗号処理部 310 と、システム 1C300 に対する外部からのアクセスを監視する監視部 320 と、副記憶部 340 及び監視部 320 に電源を供給し、監視部 320 から電源遮断指示があると副記憶部 340 への電源供給を遮断する機能を有する内部電源部 330 と、内部電源部 330 の電源供給により暗号化鍵／復号化鍵を保持する副記憶部 340 とを組み込み、かつこれらを 1 チップ化して構成し、暗号化鍵／復号化鍵を記憶する副記憶部 340 は内部電源部 330 によりバックアップされ、監視部 320 が不正アクセスを検知するとバックアップを遮断して副記憶部 340 の内容を消去するようにしたので、プログラムやデータを暗号化されていない状態で扱う箇所をチップ内（システム 1C300 内）に限定することができ、かつシステム 1C300 外部の外部記憶部 200 に記憶しておくときは暗号化することができる。暗号化されたデータは、復号化のための鍵がなければ解読することが非常に困難であるため現在の技術では外部からの攻撃に対して安全であると言える。

【0049】すなわち、システム 1C300 内に暗号処理部 310、監視部 320、内部電源部 330 及び副記憶部 340 を組み込み 1 チップ化された構成であることから、副記憶部 340 等を単独で取り出すことは極めて困難であることに加え、暗号化鍵／復号化鍵を記憶する副記憶部 340 は内部電源部 330 によりバックアップされ、監視部 320 が不正アクセスを検知すると瞬時に電源バックアップを遮断して副記憶部 340 の内容を消去するため外部からの不正使用は極めて困難である。

【0050】上述したように、復号化のための鍵が強固に保護されていることから、仮に外部記憶部 200 からプログラムやデータが読み出されたり、外部記憶部 200 とシステム 1C300 間の信号線 150 上を通信する

プログラムやデータが読み取られることがあっても、暗号化されたデータを解読することは非常に困難である。  
【0051】以上のことからプログラムやデータの解析・改竄による不正使用の脅威からシステムの安全を保持することができる。

【0052】また、システム1C300内部に電源部を持つことにより、使用（通電）していないときでもシステム1C300単体での監視が可能である。また、内部電源が切れる時には、暗号化鍵を記憶している副記憶部340のデータを消去するようにしているため、暗号化鍵の漏洩を防ぐことができる。

【0053】第2の実施形態  
本発明の第2の実施形態に係るシステム1Cは、基本構成は前記図1及び図2と同じであり、第1の実施形態とは副記憶部340のデータ消失方法が異なる。以下、第1の実施形態と異なる部分についての説明する。

【0054】本実施形態に係るシステム1Cは、前記図1及び図2に示す監視部320が、システム1C300に対する外部からのアクセスを常に監視し、システム1C300に対して不正なアクセスがあった時、まず、副記憶部340のデータを破壊するようにデータを書き換え、その後、内部電源部330に電源遮断指示を出して副記憶部340への電源供給を遮断させ、副記憶部340の暗号化鍵/復号化鍵を消去する。

【0055】例えば、暗号化鍵として、64bitのDESを用いている場合、監視部320が不正アクセスを検知した時、副記憶部340が記憶しているデータの任意のbit（わずかに1bitでもよい）を書き換え、その後、副記憶部340の暗号化鍵/復号化鍵を消去する。一般に、暗号化鍵において、1bitでもデータが書き換えられると全く異なる鍵となり殆ど完全にデータを破壊することができ。

【0056】図4は本実施形態に係る監視手段350の監視部320の監視動作を示すフローチャートであり、前記図3に示すフローと同一ステップには同一符号を付して重複部分の説明を省略する。

【0057】図4において、ステップS1で内部電源部330の出力電圧が所定値以下のとき、ステップS2で不正アクセスがあったとき、あるいはステップS2でセンサ入力に異常があったときは、システム1Cに対して外部からプログラムやデータの解析・改竄のための不正使用が行われたと判断してステップS11に進む。

【0058】ステップS11では、副記憶部340のデータを破壊するように副記憶部340が記憶しているデータの任意のbitを書き換えて強制的にデータを削除する。

【0059】次いで、ステップS15で内部電源部330に電源遮断を指示し、内部電源部330から副記憶部340への電源供給を遮断する。これにより、副記憶部

34内の暗号化鍵/復号化鍵を消去する。

【0060】以上説明したように、第2の実施形態に係るシステム1Cは、監視部320が、システム1Cに対する外部からのアクセスを常に監視し、システム1Cに対して不正なアクセスがあった時、まず、副記憶部340のデータを破壊するようにデータを書き換え、その後、内部電源部330に電源遮断指示を出して副記憶部340への電源供給を遮断させ、副記憶部340の暗号化鍵/復号化鍵を消去するように構成したので、第1の実施形態で述べた効果をより一層高めシステムの安全を保持することができる。

【0061】すなわち、第1の実施形態では、内部電源供給を遮断して、暗号化鍵を記憶している副記憶部340のデータを消去するようにしている。副記憶部340は、内部電源部330からの電源供給が絶たれたと、極めて短い時間に記憶内容が消失する。しかし、最近では、メモリを低温保存すること等により電源供給がなくなったメモリからデータを読み取ることが可能になっている。また、内部電源部330からの電源供給を遮断して副記憶部340の記憶内容が失われる、極めて短い時間

にデータを読み取ることも考えられる。  
【0062】そこで、第2の実施形態では、システム1Cに対して不正なアクセスがあった時、副記憶部340の記憶内容を破壊するようにデータを書き換え、データを強制的に削除することにより、上記暗号化鍵の漏洩の可能性を排除することができる。

【0063】なお、第2の実施形態では、システム1Cに対して不正なアクセスがあった時、副記憶部340のデータを破壊するようにデータを書き換え、さらに、副記憶部340への電源供給を遮断させて、副記憶部340の暗号化鍵/復号化鍵を消去するようにしているが、上記副記憶部340の記憶内容の書き換えのみであってもよい。この場合は、内部電源部330の組み込みが必須ではなくなる効果を得ることができ。

【0064】したがって、このような優れた特長を有するシステム1Cを、電子マネーシステムの電子マネーの決済部に用いられるシステム1Cに適用すれば、プログラムやデータの解析・改竄による不正使用の脅威からシステムの安全性を格段に向上させることができる。

【0065】なお、上記各実施形態に係るシステム1Cを、上述したような電子マネーの決済部に適用することもできるが、勿論これには限定されず、演算処理部、主記憶部、通信制御部を行う通信処理部を備え、外部記憶装置とアクセス可能な集積回路装置であれば全ての装置に適用可能であること言うまでもない。

【0066】また、上記各実施形態に係るシステム1Cでは、信号線150を經由した外部記憶部200には限定されず、外部装置の種類及び数、接続のインターフェースはどのようなものであってもよいことは勿論である。



【0067】さらに、上記システムIC、各部を構成する回路の種類、接続数、接続形態などは上述の実施形態に限られないことは言うまでもない。

【0068】

【発明の効果】本発明に係る集積回路装置では、外部記憶装置からのプログラム及びデータを復号化するとともに、外部記憶装置にデータを書き出す時にデータの暗号化を行う暗号処理部と、内部電源部の電源供給により暗号化鍵／復号化鍵を保持する副記憶部と、集積回路装置に対する外部からのアクセスを監視し、不正アクセスを検知すると電源遮断指示する監視部と、副記憶部に電源を供給し、監視部から電源遮断指示があると副記憶部への電源供給を遮断する機能を有する内部電源部とを備えて構成したので、プログラムやデータの解析・改竄による不正な使用の脅威からシステムの安全を保持することができる。

【0069】本発明に係る集積回路装置では、外部記憶装置からのプログラム及びデータを復号化するとともに、外部記憶装置にデータを書き出す時にデータの暗号化を行う暗号処理部と、暗号化鍵／復号化鍵を保持する副記憶部と、集積回路装置に対する外部からのアクセスを監視し、不正アクセスを検知すると副記憶部の記憶内

容を書き換える監視部とを備えて構成したので、プログラムやデータの解析・改竄による不正な使用の脅威からシステムの安全を保持することができる。

【図面の簡単な説明】

【図1】本発明を適用した第1の実施形態に係る集積回路装置の構成を示すブロック図である。

【図2】上記集積回路装置の監視手段の構成を詳細に示すブロック図である。

【図3】上記集積回路装置の監視部の監視動作を示すフローチャートである。

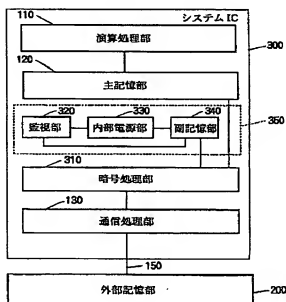
【図4】本発明を適用した第2の実施形態に係る集積回路装置の監視部の監視動作を示すフローチャートである。

【図5】従来の集積回路装置の構成を示すブロック図である。

【符号の説明】

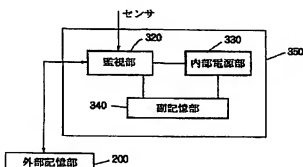
110 演算処理部、120 主記憶部、130 通信処理部、150 信号線、200 外部記憶部（外部記憶装置）、300 システムIC（集積回路装置）、310 暗号処理部、320 監視部、330 内部電源部、340 副記憶部、350 監視手段

【図1】

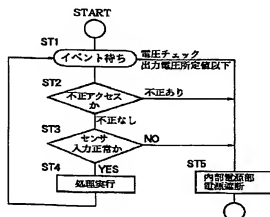


システムICの構成図

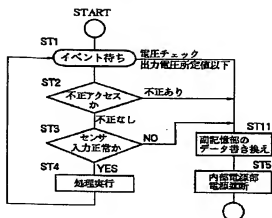
【図2】



【図3】



【図 4】



【図 5】

